United States Environmental Protection Agency
Office of Solid Waste and Emergency Response
EPA-540-F-99-008
OSWER-9360.8-18FS
PB 99-963222
June 1999

Y2K Issues in the Oil Program

Office of Emergency and Remedial Response

Quick Reference Fact Sheet

Abstract

The Year 2000 (Y2K) problem has been identified as a potential glitch in existing computer databases, software applications, and hardware chips that could cause the disruption of, or completely stop computer operations. This fact sheet discusses how the Y2K problem could affect the Oil Program, EPA's requirements for Y2K compliance, and what the Oil Program is currently doing about Y2K.

What is the Y2K Problem?

The Year 2000 (Y2K) problem or "millennium bug" is the result of cost- and space-saving computer programming practices that originated when memory space and systems were at a premium. In an effort to save space when developing software and microchips, programmers often used a two-digit date code (e.g., 99) rather than four digits (e.g., 1999). Use of the two-digit coding system has created the potential for computers and microchips to mistakenly interpret a two-digit date code of "00" as the year 1900 rather than 2000. This may cause the computer, device, or system to shut down or behave unpredictably or erratically. There are in general two types of affected systems:

- Information Technology (IT) - complex hardware and software computer systems, and
- Embedded Controls - simple microprocessors (microchips) with hard-coded programming.

Y2K malfunctions could result in major disruptions in business operations, make emergency response more difficult, or even pose threats to human health or the environment.

How Could Y2K Affect the Oil and Gas Industry?

Oil and gas industries across the U.S. are subject to Y2K vulnerabilities both within their own operations and organizations, and systems outside of their immediate control. Internal Y2K concerns for the oil and gas industry include computer hardware and software, and also systems such as automated controls that manage pumps, natural gas compressors, wellheads, and air compressors. The steps of the oil delivery process, including production, processing, refining, and storage, often use computerized or embedded electronic controls. These controls are numerous, widespread, and have the potential to be affected by Y2K and other associated dates. External considerations for oil and gas industries include the Y2K readiness of their suppliers of raw materials, telecommunications, water, and electricity. Disruptions in links to these external organizations may not only cause breaks in oil and gas service, but could potentially cause harm to human health or the environment.

What are EPA's Y2K Requirements?

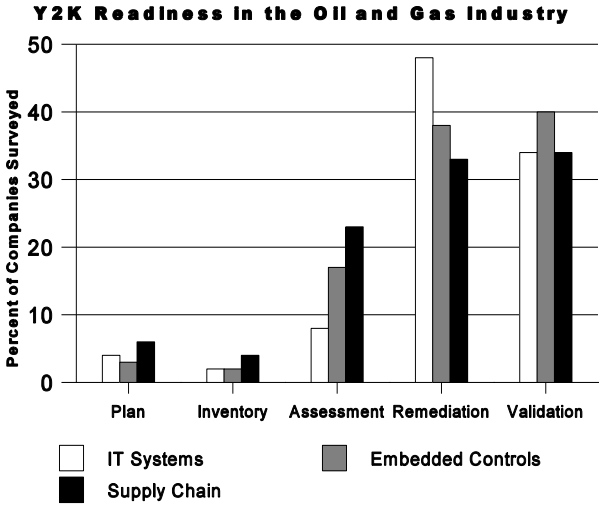
EPA requires owners and operators of all facilities which handle hazardous substances, including oil and gas facilities, to take necessary steps to prevent and mitigate accidental releases under the General Duty Clause of the Clean Air Act (CAA Section 112(4)(1)). This includes releases caused by Y2K failures. Additionally, EPA's Risk Management Program (RMP) Rules (CAA Section 112(r)(7)) regarding consideration of alternative release scenarios includes releases related to Y2K problems (e.g., loss of utilities, interruption of raw material delivery, or failure of monitoring equipment).

To assist facilities in preparing for Y2K, EPA has developed an enforcement policy to encourage facilities to test systems and equipment for Y2K problems which might adversely affect environmental compliance. Under the policy (published on the Internet at www.epa.gov/year2000), EPA stated its intent to waive 100 percent of the civil penalties that might otherwise apply, and to recommend against criminal prosecution, for environmental violations caused during specific tests that are designed to identify and eliminate Y2K-related malfunctions. *The policy also states*

that the civil penalty waiver and recommendation against criminal prosecution are limited to testing-related violations disclosed to EPA by February 1, 2000, and are subject to certain conditions, such as the need to design and conduct the tests well in advance of the dates in question, the need to conduct the tests for the shortest possible period of time necessary, the need to correct any testing-related violations immediately, and other conditions to ensure that protection of human health and the environment is not compromised.

Oil and Gas Industry Progress with Y2K Issues

Oil and gas industries have been taking the Y2K problem very seriously. Extensive efforts continue within the industry to eliminate Y2K errors that may result in either harmful and costly oil spills or prevention of delivery of product to consumers. Several trade organizations have conducted a series of surveys to gauge the oil and gas industry's performance. The results of the latest survey in January 1999, can be viewed on the Internet at http://www.api.org/ecit/y2k/. The survey included responses from 1,000 oil and gas companies. The following chart shows the percent of companies surveyed who reported to be in each of five readiness phases for their information technology systems, embedded control systems, and supply chain systems.



Source: American Petroleum Institute, January 1999 Y2K Readiness Survey

How is EPA's Oil Program Preparing for Y2K?

EPA's Emergency Response Program, including the Oil Program, is addressing Y2K issues and readiness from several directions including:

- Working with the oil and gas industry and collecting information on its Y2K efforts;
- Ensuring EPA's Emergency Response Program is Y2K compliant; and
- Preparing for increased emergency activities.

To serve these purposes, EPA's Emergency Response Program has formed a Y2K Workgroup that includes regional personnel and members of the Environmental Response Team, the Technology Innovation Office, the Chemical Preparedness and Prevention Office, and the Office of Radiation and Indoor Air.

To keep EPA informed of and involved in Y2K issues in the oil and gas industry, members of this workgroup coordinate with the regional EPA staff member responsible for outreach to the public regarding Y2K issues. In some cases, the workgroup member is the outreach coordinator. Members attend public and private sector meetings and bring information back to the workgroup. Additionally, the group meets to monitor the Emergency Response Program's Y2K readiness — pooling and sharing information among the Regions and organizations, reporting on section status, and developing guidance. The group is also working to build communications with local responders in anticipation of potential wide scale emergency activity. Currently, the workgroup's monthly conference calls are being coordinated by EPA Headquarters.

Internally, each EPA region is addressing its information technology and facility systems with support from Headquarters. Systems that could potentially be affected include: response equipment, communication equipment, field information technology, office equipment, building systems (e.g., security and HVAC), personnel availability, and engineered systems at hazardous waste sites.

Similar to the oil and gas industry, EPA's Oil and Emergency Response Programs may be subject to external vulnerability. This includes systems beyond the immediate control of EPA that have the potential to effect emergency or remedial response and may pose a threat to human health or the environment. Because these problems are not always obvious, steps are being taken to identify and prioritize these systems. Broad categorizations of these external factors include power delivery, transportation, communication, supply chains, water, wastewater, HAZMAT, and medical functions. While these items may not pose a direct threat to the environment, they could represent infrastructure failures and divert response resources.

Guidelines for Addressing Problems

Addressing Y2K issues is a multistep process for any organization. Documentation of the process, which may include writing regular progress reports and/or managing an inventory compliance database, is important in order to maximize efficiency and eliminate redundancies. Preparing for Y2K should include the following steps:

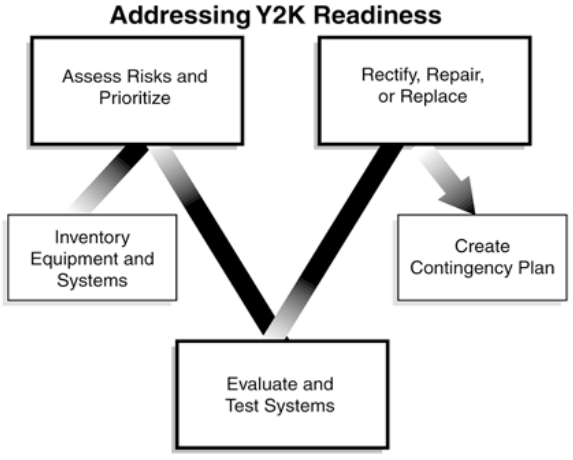
1. *Inventory Equipment and Systems* - All equipment which is suspected to contain hardware, software, or embedded chips that could be date sensitive should be included in the inventory.

2. *Assess Risks and Prioritize* - Systems that are critical to operations should be identified and prioritized accordingly versus other equipment which may have less impact if affected.

3. *Evaluate and Test Systems* - Initially, contact should be made with manufacturers in regards to their system's or software's compliance. Several programs have been developed to test computer systems for Y2K compliance. These diagnostic tools are generally used by technical experts. Testing databases may require examination of customized programs and the data in the database. Equipment should still be tested directly if possible, even when given assurances of compliance by the manufacturer.

4. *Rectify, Repair, or Replace* - Software upgrades or patches may be available through the manufacturer or online. Some equipment may be able to be manipulated manually or may need complete replacement.

5. *Create Contingency Plans* - Contingency plans should be developed that address internal and external vulnerabilities. Issues to address include communications, resource needs, deployment, and staffing.



Once systems have been tested and corrected, they should be reevaluated to ensure compliance. Additionally, measures should be taken to ensure that corrected systems are not recontaminated through installation of new, potentially non-compliant hardware or software. The inventory should be maintained and updated as new information is available either through the manufacturer or testing.

Critical Y2K Dates

Besides January 1, 2000, there are several other dates which could be problematic for computer or embedded chip systems. These dates should be considered during the testing and planning steps of Y2K readiness.

Critical Y2K Dates

Date	Issue
June 1, 1999	Fiscal year start in some countries
August 21, 1999	GPS rollover date
September 9, 1999	9999 used as an "end of file" or "infinity" code
October 1, 1999	U.S. Federal fiscal year 2000 start date
January 1, 2000	Rollover halting or disrupting systems and devices
February 29, 2000	Systems may not recognize leap year
October 10, 2000	First time the date field uses maximum length
December 31, 2000	Some systems may not recognize the 366th day of the year

Informational Resources

Widespread concern about Y2K problems has led many organizations to publish information that can be helpful in preparing for Y2K. Y2K Information can be found on these websites:

EPA http://www.epa.gov/year2000/

Federal Energy Regulatory Commisssion - Oil and Gas Sector http://www.ferc.fed.us/y2k/index.html

EPA's Office of Solid Waste and Emergency Response http://clu-in.org/y2k.htm

Occupational Safety and Health Administration http://www.osha.gov/Y2knews.pdf

National Institute of Standards and Technology http://www.nist.gov/y2k

President's Council on Year 2000 http://www.y2k.gov

Year 2000 Information Center
http://www.year2000.com

U.S. Federal Government Gateway for Y2K Information Directories
http://www.itpolicy.gsa.gov/mks/yr2000/y2khome.htm

Additional information can also be obtained by calling:

The Emergency Planning and Community Right-To-Know Hotline: (800)424-9346 or (703)412-9810
TDD (800)553-7672, M-F, 9 AM to 6 PM, EST

The President's Council on Year 2000 Conversion free information hotline: (800)USA-4-Y2K